

THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Wenxiao He	§	Art Unit:	2617
		§		
Serial No.:	10/783,637	§	Examiner:	Erika A. Gary
		§		
Filed:	February 20, 2004	§	Conf. No.:	7335
		§		
For:	Method And Apparatus For	§	Atty. Dkt.	200311424-1
	Registering A Mobile Node	§	No.:	(HPC.0698US)
	With A Home Agent	§		

Mail Stop **Appeal Brief-Patents**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF**

Sir:

The final rejection of claims 1-40 is hereby appealed.

## **TABLE OF CONTENTS**

REAL PARTY IN INTEREST .....	3
RELATED APPEALS AND INTERFERENCES.....	4
STATUS OF CLAIMS .....	5
STATUS OF AMENDMENTS .....	6
SUMMARY OF CLAIMED SUBJECT MATTER .....	7
GROUND OF REJECTION TO BE REVIEWED ON APPEAL .....	10
ARGUMENT.....	11
CLAIMS APPENDIX.....	17
EVIDENCE APPENDIX.....	25
RELATED PROCEEDINGS APPENDIX.....	26

**REAL PARTY IN INTEREST**

The Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

### **RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences.

### **STATUS OF CLAIMS**

The application was originally filed with claims 1-40. Claim 17 was amended during prosecution. Claims 1-40 have been finally rejected and are the subject of this appeal.

### **STATUS OF AMENDMENTS**

All amendments have been entered.

## **SUMMARY OF CLAIMED SUBJECT MATTER**

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

Independent claim 1 recites a method for registering a mobile node with a home agent comprising:

- determining a home agent (Instant specification in at least paragraphs 11, 13, 14, 19, 20, 24, and 35 and FIG. 1, element 5, FIG. 4, FIG. 5, element 240, FIG. 8, element 420, FIG. 9, element 420);

- establishing between the mobile node and the determined home agent a security tunnel having associated with said tunnel a single security association (Instant specification in at least paragraphs 11, 13, 16-18, 21, 25-26, 34, 36-38, 40 and FIG. 1, element 10, FIG. 2, FIG. 4, element 120, FIG. 5, element 245, FIG. 8, element 425, FIG. 9, element 425); and

- registering the mobile node with the home agent using the security tunnel (Instant specification in at least paragraphs 11, 13, 19, 20, 22, 24, 30, 36 and FIG. 1, element 15, FIG. 3, FIG. 5, element 210, FIG. 7, element 210, FIG. 9, element 430).

Per the Summary section of the Instant specification, "Registration occurs when a home agent is determined and a security tunnel having a single security association is established between the home agent and the mobile node. The mobile node is then registered [by] the mobile node using the security tunnel."

Independent claim 9 recites a mobile node comprising:

- mobile communication interface capable of communicating with a mobile network (Instant specification in at least paragraphs 24, 32, 35, and FIG. 5, element 205, FIG. 8, element 410, FIG. 9, element 410);

- home agent determination unit capable of identifying a home agent (Instant specification in at least paragraphs 11, 13, 14, 19, 20, 24, and 35 and FIG. 1, element 5, FIG. 4, FIG. 5, element 240, FIG. 8, element 420, FIG. 9, element 420);

- security tunneling unit capable of establishing and maintaining a security tunnel between the mobile node and an identified home agent, wherein an established security tunnel uses a single security association descriptor for one or more data paths (Instant specification in at least

paragraphs 11, 13, 16-18, 21, 25-26, 34, 36~38, 40 and FIG. 1, element 10, FIG. 2, FIG. 4, element 120, FIG. 5, element 245, FIG. 8, element 425, FIG. 9, element 425); and

registration unit capable of registering the mobile node with an identified home agent using an established security tunnel (Instant specification in at least paragraphs 11, 13, 19, 20, 22, 24, 30, 36 and FIG. 1, element 15, FIG. 3, FIG. 5, element 210, FIG. 7, element 210, FIG. 9, element 430).

Independent claim 17 recites a mobile node comprising:

processor for executing an instruction sequence (Instant specification in at least paragraph 32, and FIG. 8, element 400);

memory for storing an instructions sequence (Instant specification in at least paragraph 32, and FIG. 8, element 405);

mobile communications interface for communicating with a mobile network (Instant specification in at least paragraphs 24, 32, 35, and FIG. 5, element 205, FIG. 8, element 410, FIG. 9, element 410);

instruction sequences stored in the memory including: home agent determination instruction sequence that, when executed by the processor, minimally causes the processor to identify a home agent for the mobile node (Instant specification in at least paragraphs 11, 13, 14, 19, 20, 24, and 35 and FIG. 1, element 5, FIG. 4, FIG. 5, element 240, FIG. 8, element 420, FIG. 9, element 420);

security tunneling instruction sequence that, when executed by the processor, minimally causes the processor to establish a security tunnel from the mobile node to an identified home agent where the security tunnel uses a single security association descriptor to secure a plurality of data paths (Instant specification in at least paragraphs 11, 13, 16-18, 21, 25-26, 34, 36-38, 40 and FIG. 1, element 10, FIG. 2, FIG. 4, element 120, FIG. 5, element 245, FIG. 8, element 425, FIG. 9, element 425); and

registry instruction sequence that, when executed by the processor, minimally causes the processor to register the mobile node with an identified home agent using the established security tunnel (Instant specification in at least paragraphs 11, 13, 19, 20, 22, 24, 30, 36 and FIG. 1, element 15, FIG. 3, FIG. 5, element 210, FIG. 7, element 210, FIG. 9, element 430).



Independent claim 25 recites a computer readable medium having imparted thereon instruction sequences for registering a mobile node with a home agent including (Instant specification in at least paragraph 33):

home agent determination instruction sequence that, when executed by a processor, minimally causes the processor to identify a home agent for the mobile node (Instant specification in at least paragraphs 11, 13, 14, 19, 20, 24, and 35 and FIG. 1, element 5, FIG. 4, FIG. 5, element 240, FIG. 8, element 420, FIG. 9, element 420);

security tunneling instruction sequence that, when executed by a processor; minimally causes the processor to establish a security tunnel from the mobile node to an identified home agent where the security tunnel uses a single security association descriptor to secure a plurality of data paths (Instant specification in at least paragraphs 11, 13, 16-18, 21, 25-26, 34, 36-38, 40 and FIG. 1, element 10, FIG. 2, FIG. 4, element 120, FIG. 5, element 245, FIG. 8, element 425, FIG. 9, element 425); and

registry instruction sequence that, when executed by a processor, minimally causes the processor to register the mobile node with an identified home agent (Instant specification in at least paragraphs 11, 13, 19, 20, 22, 24, 30,36 and FIG. 1, element 15, FIG. 3, FIG. 5, element 210, FIG. 7, element 210, FIG. 9, element 430).

Independent claim 33 recites a mobile node comprising:

means for determining a home agent (Instant specification in at least paragraphs 11, 13, 14, 19,20,24, and 35 and FIG. 1, element 5, FIG. 4, FIG. 5, element 240, FIG. 8, element 420, FIG. 9, element 420);

means for establishing a single-security-association based security tunnel between the mobile node and a determined home agent (Instant specification in at least paragraphs 11,13,16-18,21,25-26,34,36-38,40 and FIG. 1, element 10, FIG. 2, FIG. 4, element 120, FIG. 5, element 245, FIG. 8, element 425, FIG. 9, element 425); and

means for registering the mobile node using an established security tunnel (Instant specification in at least paragraphs 11, 13, 19, 20, 22, 24, 30, 36 and FIG. 1, element 15, FIG. 3, FIG. 5, element 210, FIG. 7, element 210, FIG. 9, element 430).

**GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

- A. The issue is whether claims 1, 9, 17, 25, and 33 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Eschbach (US Patent Application Publication 2003/0088765).
- B. The issue is whether claims 1, 9, 17, 25, and 33 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Giaretta (US Patent Application Publication 2007/0230453).
- C. The issue is whether claims 3-7, 11-15, 19-23, 27-31, and 35-39 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach in view of Thubert (US Patent Application Publication 2004/0202183).
- D. The issue is whether claims 2, 10, 18, 26, and 34 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach in view of Johansson (US Patent Application Publication 2002/0080752).
- E. The issue is whether claims 8, 16, 24, 32, and 40 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach and Thubert in view of Johansson.

## ARGUMENT

- A. **The issue is whether claims 1, 9, 17, 25, and 33 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Eschbach (US Patent Application Publication 2003/0088765).**

The rejection of claims 1, 9, 17, 25, and 33 under 35 U.S.C. § 102(e) as being anticipated by Eschbach is hereby traversed. A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Claims 1, 9, 17, 25 and 33 are patentable over Eschbach because the reference fails to disclose or suggest every element of those claims.

The PTO attempts to rely on paragraph 30 of *Eschbach* for the assertion that the subject matter of claims 1, 9, 17, 25 and 33 is anticipated by the reference. This is incorrect.

Claim 1 is directed to a method for registering a mobile node with a home agent, such as when the mobile node has moved out of the home agent's subnet. Towards that end, claim 1 requires determining a home agent, establishing a security tunnel between the home agent and the mobile node, and then registering the mobile node with the home agent using the security tunnel.

Eschbach, on the other hand, is directed to a process for enabling session inter-device (SID) mobility. SID mobility, as described by Eschbach at paragraph 30, is the transfer of a session from a first destination device (i.e., a Transferring Node) to a second destination device (i.e., a Target Node) that is implicitly trusted by the Transferring Node. After the Transferring Node registers the Target Node with the Home Agent, the Home Agent then intercepts packets sent to the Transferring Node and tunnels them to the Target Node. (Eschbach, paras. [0032]-[0035]). Eschbach discloses that, during the negotiation for the transfer, the Transferring Node informs the Target Node of the Home Agent's IP address. Then, the Transferring Node requests the Agent to transfer the session to the Target Node. This request contains the Transferring and Target Nodes' IP addresses, a session key that has been encrypted using a Transferring Node/Home Agent security association, and an indication of whether further transferring of the session is permitted. The Agent authenticates whether the request came from the Transferring Node and then sets up a binding which associates the Transferring Node's IP address with the Target Node's IP address. Eschbach further discloses that the binding is valid for a finite lifetime that "may be negotiated between the Transferring Node 56 and the Agent 60 as part of

the registration process.” (Eshbach, para. [0034]). Once this registration process between the Transferring Node and the Agent is complete, then the Agent begins intercepting data packets sent to the Transferring Node’s IP address and tunnels them to the Target Node. (Eshbach, para. [0035]).

As is clear from this description, the security tunnel between the Home Agent and the Target Node is not used until *after* the Transferring Node has registered the Target Node with the Home Agent using a security association *between the Transferring Node and the Home Agent*. In other words, Eschbach does not disclose registering a mobile node with a home agent using a security tunnel that has been established *between the mobile node and the home agent*, as required by claim 1. Thus, Eschbach does not anticipate claim 1 and reversal of the rejection of claim 1 is requested.

Claims 9, 17, 25 and 33 are patentable over Eschbach for at least reasons similar to those advanced above. Accordingly, reversal of the rejection of those claims in view of Eschbach is requested.

**B. The issue is whether claims 1, 9, 17, 25, and 33 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Giaretta (US Patent Application Publication 2007/0230453).**

The rejection of claims 1, 9, 17, 25 and 33 under 35 U.S.C. § 102(e) as being anticipated by Giaretta is hereby traversed. A rejection based on 35 U.S.C. § 102 requires every element of the claim to be included in the reference, either directly or inherently. Claims 1, 9, 17, 25 and 33 are patentable over Giaretta because the reference fails to disclose or suggest every element of those claims.

Giaretta fails to disclose or suggest “registering the mobile node with the home agent **using the security tunnel**,” as required by claim 1 (emphasis added). The Final Office states that Giaretta discloses “using the security tunnel” to register the mobile node with the home agent because Giaretta “teaches that once a security association is established, the mobile node registers with the home agent [paragraph 0147].” Final Office Action, at p. 6. However, a security *association* is not a security *tunnel*. Instead, a security association simply represents security features that should be used for a data path, regardless whether that path is a transport layer or a security tunnel. (See, e.g., Specification, para. [0008]).

That the security association referenced in paragraph 0147 of Giaretta is not a security tunnel is further evident from the description set forth in paragraph 0142 of Giaretta. That paragraph discloses that the security association in paragraph 0147 is established in compliance with the IPSec-04 standard. Paragraph [0008] of the instant application explains that the IPSec transport mode---and not the IPSec tunnel mode---traditionally is used to propagate binding updates and acknowledgements. *See* Specification, at para. [0008]. Accordingly, no inference can be made that the security association in paragraph 0147 of Giaretta is being used with a security tunnel, as argued by the examiner in the Final Office action, since a security association also may be used in the transport mode. As such, Giaretta does not disclose --- explicitly or inherently --- registering a mobile node with a home node using the security tunnel, as required by claim 1.

In view of the foregoing, it is submitted that claim 1 is not anticipated by Giaretta and reversal of the rejection of claim 1 in view of Giaretta is requested.

Claims 9, 17, 25 and 33 are patentable over Eschbach for at least reasons similar to those advanced above. Accordingly, reversal of the rejection of those claims in view of Eschbach is requested.

**C. The issue is whether claims 3-7, 11-15, 19-23, 27-31, and 35-39 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach in view of Thubert (US Patent Application Publication 2004/0202183).**

The rejection of claims 3-7, 11-15, 19-23, 27-31, and 35-39 under 35 U.S.C. 103(a) as being obvious in view of Eschbach and Thubert is hereby traversed. Here, the claims are not obvious in view of Eschbach and Thubert for at least the reason that the references, either alone or in the proposed combination, do not disclose or suggest every element of the claims.

Claims 3-7 depend from claim 1. The deficiencies of Eschbach with respect to claim 1 have been discussed above. Specifically, Eschbach does not teach or suggest registering the mobile node with the home agent using the security tunnel established between the mobile node and the home agent. Thubert does not compensate for these deficiencies. In fact, the Examiner admitted in the Final Office action that Thubert was cited only for “aspects of establishing a security tunnel and conveying data using the security tunnel. These aspects are well known in the art, regardless of what entities the security tunnel is connecting.” Final Office action, at pp. 6-7.

In view of the foregoing, it is submitted that elements recited by claims 3-7 are not taught or suggested by Eschbach and Thubert---either alone or in the proposed combination. Accordingly, it is submitted that a *prima facie* case of obviousness of claims 3-7 in view of Eschbach and Thubert has not been established and, as such, reversal of the final rejection of those claims is requested.

Claims 11-15, 19-23, 27-31, and 35-39 depend from claims 9, 17, 25 and 33, respectively, and recite limitations similar to those recited in claims 3-7. Accordingly, claims 11-15, 19-23, 27-31 and 35-39 are patentable over Eschbach and Thubert for at least the same reasons discussed above with respect to claims 3-7. As such, reversal of the final rejection of claims 11-15, 19-23, 27-31 and 35-39 is respectfully requested.

**D. The issue is whether claims 2, 10, 18, 26, and 34 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach in view of Johansson (US Patent Application Publication 2002/0080752).**

The rejection of claims 2, 10, 18, 26, and 34 under 35 U.S.C. § 103(a) as being obvious in view of Eschbach and Johansson is hereby traversed. Here, the claims are not obvious in view of Eschbach and Thubert for at least the reason that the references, either alone or in the proposed combination, do not disclose or suggest every element of the claims.

Claim 2 depends from claim 1. The deficiencies of Eschbach with respect to claim 1 have been discussed above. Specifically, Eschbach does not teach or suggest registering the mobile node with the home agent using the security tunnel established between the mobile node and the home agent. Johansson does not compensate for these deficiencies. In fact, the Examiner admitted in the Final Office action that Johansson was “only relied upon to teach a security policy database.” Final Office action, at p. 7.

In view of the foregoing, it is submitted that elements recited by claim 2 are not taught or suggested by Eschbach and Johansson---either alone or in the proposed combination. Accordingly, it is submitted that a *prima facie* case of obviousness of claim 2 in view of Eschbach and Johansson has not been established and, as such, reversal of the final rejection of claim 2 is requested.

Claims 10, 18, 26, and 34 are based on claims 9, 17, 25 and 33, respectively, and recite limitations similar to those recited in claim 2. Accordingly, claims 10, 18, 26 and 34 are patentable over Eschbach and Johansson for at least the same reasons discussed above with

respect to claim 2. As such, reversal of the final rejection of claims 10, 18, 26 and 34 is respectfully requested.

**E. The issue is whether claims 8, 16, 24, 32, and 40 are unpatentable under 35 U.S.C. § 103(a) as being obvious in view of Eschbach and Thubert in view of Johansson.**

The rejection of claims 8, 16, 24, 32, and 40 under 35 U.S.C. § 103(a) as being obvious in view of Eschbach, Thubert and Johansson is hereby traversed. Here, the claims are not obvious in view of Eschbach, Thubert and Johansson for at least the reason that the references, either alone or in the proposed combination, do not disclose or suggest every element of the claims.

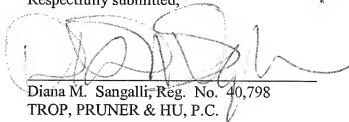
Claim 8 depends from claim 7, and indirectly from claim 1, and includes additional limitations. Thus, claim 8 is patentable over Eschbach in view of Thubert and further in view of Johansson for at least the reasons advanced above with respect to claims 1 and 7. More specifically, for the reasons discussed above, Thubert and Johansson fail to compensate for the deficiencies of Eschbach. For at least this reason, the rejection of claim 8 should be reversed.

With respect to claims 16, 24, 32 and 40, they are based on claims 9, 17, 25 and 33, respectively, and include limitations similar to those recited in claim 8. The deficiencies of Eschbach with respect to each of the base claims has been discussed above, and, as discussed above, Thubert and Johansson do not compensate for those deficiencies. Accordingly, for at least these reasons, the rejection of claims 16, 24, 32 and 40 should be reversed.

CONCLUSION

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read 'Diana M. Sangalli', is written over a horizontal line.

Date: May 5, 2009

Diana M. Sangalli, Reg. No. 40,798  
TROP, PRUNER & HU, P.C.  
1616 S. Voss Road, Suite 750  
Houston, Texas 77057  
713/468-8880 [Phone]  
713/468-8883 [Fax]



## **CLAIMS APPENDIX**

The claims on appeal are:

1. A method for registering a mobile node with a home agent comprising:  
determining a home agent;  
establishing between the mobile node and the determined home agent a security tunnel  
having associated with said tunnel a single security association; and  
registering the mobile node with the home agent using the security tunnel.
2. The method of claim 1 wherein establishing a security tunnel comprises:  
creating a security policy database for at least one of a binding update message, a return  
routability message, prefix discovery message and payload data packet; and  
associating two or more security policy databases with a security tunnel using a single  
security association.
3. The method of claim 1 wherein registering the mobile node with the home agent  
comprises:  
dispatching a binding update request to the home agent using the security tunnel; and  
receiving a binding update acknowledgement by way of a reverse path security tunnel.
4. The method of claim 1 further comprising discovering an applicable prefix for the  
home agent using the security tunnel.
5. The method of claim 1 further comprising conveying data to a correspondent node  
using the security tunnel.
6. The method of claim 1 further comprising communicating a return routability  
signal to the home agent using the security tunnel.
7. The method of claim 1 further comprising establishing a reverse path security  
tunnel having associated with said tunnel a single security association.

8. The method of claim 7 wherein establishing a reverse path security tunnel comprises creating a security policy database for at least one of a binding update message, a return routability message, prefix discovery message and payload data packet; and associating one or more security policy databases with a security tunnel using a single security association.

9. A mobile node comprising:  
mobile communication interface capable of communicating with a mobile network;  
home agent determination unit capable of identifying a home agent;  
security tunneling unit capable of establishing and maintaining a security tunnel between the mobile node and an identified home agent, wherein an established security tunnel uses a single security association descriptor for one or more data paths; and  
registration unit capable of registering the mobile node with an identified home agent using an established security tunnel.

10. The mobile node of claim 9 wherein the security tunnel unit comprises:  
security association descriptor capable of storing a security association;  
security policy descriptor capable of storing a security policy for at least one of a binding update message, a return routability message, a prefix discovery solicitation message and a payload data packet;  
messaging unit capable of formatting a secure message according to an incoming message that includes at least one of a binding update message, a return routability message, a prefix discovery message and a payload data packet and according to a security association stored in the security association descriptor and further capable of formatting a secure message using a security policy stored in any of the security policy descriptors, wherein the security policy descriptor is selected according to the type of the incoming message.

11. The mobile node of claim 9 wherein the registration unit comprises:  
binding request message unit that directs to the security tunneling unit a binding message directed to a home agent according to an indicator received from the home agent determination unit; and  
binding acknowledgement unit that receives a binding update acknowledgement from the security tunneling unit according to a tunneling packet received from the home agent using a reverse path security tunnel.
12. The mobile node of claim 9 further comprising a prefix discovery unit capable of discovering an applicable prefix for the determined home agent using the established security tunnel.
13. The mobile node of claim 9 further comprising a payload unit capable of accepting data from a client and directing it to the security tunneling unit.
14. The mobile node of claim 9 further comprising route discovery unit capable of dispatching a return routability message to the security tunneling unit.
15. The mobile node of claim 9 wherein the security tunneling unit is capable of establishing and maintaining a reverse path security tunnel between the mobile node and an identified home agent.
16. The mobile node of claim 15 wherein the security tunneling unit comprises:  
reverse path security association descriptor capable of storing a security association; reverse path security policy descriptor capable of storing a security policy for at least one of a binding update acknowledgement message, a return routability reply message, a prefix discovery advertisement message and a return payload data packet wherein the messaging unit is capable of unsecuring a secure tunneling message according to a security association stored in the reverse path security association descriptor and according to a security descriptor stored in at least one of the reverse path security policy descriptors wherein the reverse path security policy descriptor is selected according to the type of secure tunneling message received.

17. A mobile node comprising:  
processor for executing instruction sequence;  
memory for storing an instructions sequence;  
mobile communications interface for communicating with a mobile network;  
instruction sequences stored in the memory including: home agent determination  
instruction sequence that, when executed by the processor, minimally causes the processor to  
identify a home agent for the mobile node;  
security tunneling instruction sequence that, when executed by the processor, minimally  
causes the processor to establish a security tunnel from the mobile node to an identified home  
agent where the security tunnel uses a single security association descriptor to secure a plurality  
of data paths; and  
registry instruction sequence that, when executed by the processor, minimally causes the  
processor to register the mobile node with an identified home agent using the established security  
tunnel.

18. The mobile node of claim 17 wherein the security tunneling instruction sequence  
causes the processor to establish a security tunnel by minimally causing the processor to create a  
single security association that can be used by a plurality of data paths, including, but not limited  
to data paths for a binding update message, a return routability message, a prefix discovery  
message and a payload data packet.

19. The mobile node of claim 17 wherein the registry instruction sequence causes the  
processor to register the mobile node by minimally causing the processor to dispatch a binding  
update request to an identified home agent using a security tunnel established by the processor  
when it executes the security tunneling instruction sequence.

20. The mobile node of claim 17 further comprising a prefix discovery instruction  
sequence that, when executed by the processor, minimally causes the processor to discover a  
prefix for an identified home agent using a security tunnel established by the processor when it  
executes the security tunneling instruction sequence.

21. The mobile node of claim 17 further comprising a payload instruction sequence that, when executed by the processor, minimally causes the processor to direct a payload data packet to an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

22. The mobile node of claim 17 further comprising a return path verification instruction sequence that, when executed by the processor, minimally causes the processor to direct a return routability message to an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

23. The mobile node of claim 17 wherein the security tunneling instruction sequence further minimally causes the processor to establish a reverse path security tunnel capable of carrying a plurality of data paths using a single security association.

24. The mobile node of claim 23 wherein the security tunneling instruction sequence, when executed by the processor, minimally causes the processor to establish a reverse path security tunnel by: creating a security policy database for at least one of a binding update message, a return routability message, prefix discovery message and payload data packet; and associating one or more security policy databases with a reverse path security tunnel using a single security association.

25. A computer readable medium having imparted thereon instruction sequences for registering a mobile node with a home agent including:

home agent determination instruction sequence that, when executed by a processor, minimally causes the processor to identify a home agent for the mobile node;

security tunneling instruction sequence that, when executed by a processor, minimally causes the processor to establish a security tunnel from the mobile node to an identified home agent where the security tunnel uses a single security association descriptor to secure a plurality of data paths; and

registry instruction sequence that, when executed by a processor, minimally causes the processor to register the mobile node with an identified home agent.

26. The computer readable medium of claim 25 wherein the security tunneling instruction sequence causes a processor to establish a security tunnel by minimally causing the processor to create a single security association that can be used by a plurality of data paths, including, but not limited to data paths for a binding update message, a return routability message, a prefix discovery message and a payload data packet.

27. The computer readable medium of claim 25 wherein the registry instruction sequence causes the processor to register the mobile node by minimally causing the processor to dispatch a binding update request to an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

28. The computer readable medium of claim 25 further comprising a prefix discovery instruction sequence that, when executed by the processor, minimally causes the processor to discover prefix for an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

29. The computer readable medium of claim 25 further comprising a payload instruction sequence that, when executed by the processor, minimally causes the processor to direct a payload data packet to an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

30. The computer readable medium of claim 25 further comprising a return path verification instruction sequence that, when executed by the processor, minimally causes the processor to direct a return routability message to an identified home agent using a security tunnel established by the processor when it executes the security tunneling instruction sequence.

31. The computer readable medium of claim 25 wherein the security tunneling instruction sequence further minimally causes the processor to establish a reverse path security tunnel capable of carrying a plurality of data paths using a single security association.

32. The computer readable medium of claim 31 wherein the security tunneling instruction sequence, when executed by the processor, minimally causes the processor to establish a reverse path security tunnel by: creating a security policy database for at least one of a binding update message, a return routability message, prefix discovery message and payload data packet; and associating one or more security policy databases with a reverse path security tunnel using a single security association.

33. A mobile node comprising: means for determining a home agent; means for establishing a single-security-association based security tunnel between the mobile node and a determined home agent; and means for registering the mobile node using an established security tunnel.

34. The apparatus of claim 33 wherein the means for establishing a single-security association based security tunnel comprises means for associating a plurality of security policy databases with a single security association.

35. The apparatus of claim 33 wherein the means for registering the mobile node comprises: means for dispatching a binding update message to an identified home agent using an established security tunnel; and means for receiving a binding update acknowledgement by way of a reverse path security tunnel.

36. The apparatus of claim 33 further comprising a means for discovering an applicable prefix for the home agent using an established security tunnel.

37. The apparatus of claim 33 further comprising a means for conveying data to a correspondent node using an established security tunnel.

38. The apparatus of claim 33 further comprising a means for communicating a return routability signal to a determined home agent using an established security tunnel.

39. The apparatus of claim 33 further comprising a means for establishing a reverse path single-security-association based security tunnel.

40. The apparatus of claim 39 wherein the means for establishing a reverse path security tunnel comprises means for associating a plurality of security policy databases with a single security association.



## **EVIDENCE APPENDIX**

None.

**RELATED PROCEEDINGS APPENDIX**

None.